

## **AMENDMENTS TO THE SPECIFICATION**

### **Please amend the paragraph starting on page 7, line 20 as follows:**

We now describe the main process of IAPM, as show in the right-hand side of FIG. 7. Having used the key K2 and the nonce R to derive offsets  $Z[0]$ , ...,  $Z[m+1]$ , encipher R, now using key K1, to determine an enciphered R-value,  $C[0] = E_{K1}(R)$ . Now, for each  $i \in [1..m]$ , message block  $M[i]$  is xored with offset  $Z[i]$ , the result is enciphered using E (keyed by K1), and the resulting block is xored once again with offset  $Z[i]$ , yielding a ciphertext block  $C[i]$ : that is, for each  $i \in [1..m]$ , let  $C[i] = Z[i] \oplus E_{K1}(M[i] \oplus Z[i])$ . Call  $C = C[1] \dots C[m]$  the ciphertext core. Next, compute a checksum, Checksum, by xoring together the message blocks:  $\text{Checksum} = M[1] \oplus \dots \oplus M[m]$ . Next, form an authentication tag, Tag, by xoring the checksum with ~~offset  $Z[m+1]$~~  ~~offset  $M[m+1]$~~ , enciphering the result with  $E_{K1}$ , and xoring the resulting block with offset  $Z[0]$ :  $\text{Tag} = Z[0] \oplus E_{K1}(\text{Checksum} \oplus Z[m+1])$ . The complete ciphertext specifies  $C[0]$ , ciphertext core  $C = C[1] \dots C[m]$ , and authentication tag Tag.

### **Please amend the paragraph starting on page 17, line 2 as follows:**

FIG. 6 depicts the IACBC-IAPM scheme of Jutla.

### **Please amend the paragraph starting on page 17, line 2 as follows:**

FIG. 7 depicts the IAPM-IACBC scheme of Jutla.